REMARKS

The Examiner's office action rejects claims 35-41 of this application as unpatentable over US Published Patent Application 2003/0126445 by Wehrenberg.

Summary of published US Published Patent Application US 2003/0126445 A1 by Wehrenberg:

This publication provides for the copy protection of data (also called content or video image) utilizing a watermark and a permission key, wherein the value of the watermark designates different levels of copy protection, and wherein the permission key can be encrypted.

As long as a watermark is included in the content, and as long as a permission key is provided, the recipient of a content-transmission is allowed to make a copy of the content. After copying the content, the permission key is discarded.

The permission key may be formulated to correspond to the watermark so that a receiving device can compare the permission key to the watermark in order, to ensure that the permission key is correct for that particular content.

The permission key may be a pseudo-random code, with a seed that is known to both the content-provider and the receiving-device.

Alternately, the permission key may be a constant value, but an encryption key may be varied over time and the encryption key can be transmitted to the receiving-device over a different medium such as the phone lines.

The permission key is sent along with the content in order to allow copies (or one copy) to be made. The watermark is incorporated into the content to signify that the content is copy protected.

When a receiver-device receives a transmitted-content along with an encoded watermark, the receiver-device checks to see if a permission key is included to authorize copying of the transmitted-content. If a permission key is included, viewing and/or recording of the transmitted-content is permitted. The permission key is never stored or recorded for more than a short time interval. Rather, the permission key is discarded after a short time interval.

If the content is stored on a recording-medium, the permission key is not included in the stored content unless the purchaser of the recording-medium is allowed to make a backup-copy

of the content. However, when a permission key is included, the permission key cannot be copied onto the backup-copy.

(Note that in FIG. 3A all numbers must be increased by 10 in order to correspond to the numbers used in the specification. That is, the figure's image 60 is called image 70 in the specification. FIG. 3B does not appear to be described in the specification.)

FIG. 3A shows how a watermark and a permission key are added to a transmission. An original video image 60 is provided to a watermark encoder 62, and an MPEG encoder 63 compresses the watermarked video image, and then provides the MPEG compressed image and encoded watermark to a transmitter 65. A permission key encryptor 66 provides an encrypted permission key to transmitter 65. Transmitter 65 then combines the compressed image and encoded watermark with the encrypted permission key into a single data stream that is transmitted by antenna 70.

FIG. 6A shows transmitted video and permission key information 225 that includes a permission key packet 230 and video information packets 231.

FIG. 4 shows a receiving system for receiving a transmission, and FIG. 8 is a flow chart that shows the operation of a recording-device that receives the transmission.

In FIG. 8 a watermark is extracted from a received-content at step 404. If a watermark is not extracted, the N output of step 406 allows recording of the received-content at step 414. If a watermark is extracted, the Y output of step 406 enables step 408 to determine if a permission key is also received.

If a permission key is not received, recording is not permitted. If a permission key is received, step 410 compares the watermark to the permission key, and step 412 ensures that the watermark and permission key correspond to each other. If the watermark and permission key match, the Y output of step 412 enables step 414 to permit recording. If they do not match, the N output of step 412 enables step 416 so that recording is not permitted.

With reference to FIG. 4, a receiver 100 includes (1) a permission key extractor 108 that supplies an encrypted permission key to an interface 112, and (2) an MPEG decoder 110 that supplies an MPEG compressed video image and encoded watermark to interface 112, these two signals being applied to the controller 132 of a recording-device 130. (The details of controller 132 are shown in FIG. 5.)

Initially controller 132 verifies that a watermark is present and/or the value of the watermark. After detecting a watermark, controller 132 determines if a permission key has been transferred, and if a permission key is present, controller 132 compares the permission key to the watermark to ensure that they correspond to each other.

When controller 132 receives a valid permission key that corresponds to the received watermark, controller 132 provides the MPEG compressed content to recording mechanism 134 for recording of the video image and the watermark on DVD disc 140.

FIG. 5 shows that FIG. 4's controller 132 receives (1) the MPEG compressed content, (2) the encoded watermark, and (3) the encrypted permission key from FIG. 4's interface 112.

In controller 132 shown in FIG. 5, a comparator 140 compares a permission key that is received from store 138 to the watermark that is received from a watermark decoder 142 in order to generate a validation code that determines whether the transmitted content may be passed along to FIG. 4's recording-device 130 for recording onto recording medium 140.

Argument for the patentability of presently-amended claims 35-41:

The cited publication to Wehrenberg teaches the following technical features:

(1) Using a watermark (WM) and a Permission Key (PK), a copying of a data-content can be permitted if both the WM and the PK are present.

(2) The PK may be transmitted with the data-content, and it may be selected from the same value with the WM, quasi randomly, or constant, while updating an Encryption key according to time-elapse.

(3) The PK is abandoned after receiving the data-content, and a copy can not be associated by the PK, so that additional copying after the first copy is not permitted.

Important features of the present invention are to provide WM detection in a scrambler/descrambler that is physically disposed outside of a device such as a digital video disc (DVD) drive. The present invention provides this important function so as to not provide a chance for a signal-falsification in which a copy-inhibition signal is modified to become a copy-permission signal.

The chance of such a signal-falsification is present when a permission/inhibition signal for the copy operation is obtained from the detection of a WM that is transmitted from the DVD drive to an MPEG decoder.

It may be possible to dispose a WM detector in a DVD drive in order to minimize this chance for signal-falsification. However, a DVD drive includes many parts within its quite thin body, and a DVD drive is also subject to low-cost requirements, such that it is difficult to physically attach a WM detector to the DVD drive. This results in a trade-off problem for the implementation of copy protection in the DVD drive.

The present invention provides a new and unusual arrangement that overcomes this trade-off problem by providing a WM detector in a scrambler/descrambler that is physically outside of the DVD drive by providing scrambling/descrambling steps between detection of the WM and the decoding/encoding of the MPEG data content.

The Examiners' cited publication US 2003/0126445 does not teach these features of the present invention.

Above all, the present invention provides the new and unusual functions of the presently amended claims as is described below:

(1) The omission of a physical space within the DVD drive that is devoted to detecting falsification.

(2) In the other words, omission of the falsification that is provided in set-top box device 110 and playback device 130 that are shown in the prior scheme of FIG. 1 of the present application.

(3) Omission of a PK which must be created separately and then attached to the data-contents after encryption of the PK, which requirement degrades the merit of the WM.

US 2003-0126445 by Wehrenberg teaches copy protection by a scrambling technique shown by route A of Wehrenberg's FIG. 7, for example as described in paragraphs 0069 through 0071 thereof. In addition, FIG. 7 of Wehrenberg teaches a player 310 that includes a scrambling means so as to inhibit playback by a recording device 330.

Wehrenberg teaches ensuring one-time copying within routes B and C of FIG. 7, using a Permission Key, for example as described in paragraphs 0074 through 0076 thereof.

That is, Wehrenberg does not use a scrambling process after MPEG encoding, nor a descrambling process prior to MPEG decoding, (for example see paragraph 0072 of Wehrenberg) because neither computer 300 nor decoder 340 of FIG. 7 include a video driver card of the type described relative to the present invention.

Therefore, Wehrenberg's system must include a Permission Key other than the scrambling key means; and Wehrenberg's FIG. 7 player 310 includes a scrambling means in player 310 that includes both a scrambling technique and a Permission Key technique.

Wehrenberg fails to teach use of a scrambling process after MPEG encoding, or the use of a descrambling process prior to MPEG decoding (for example see paragraph 0072 of Wehrenberg). Also Wehrenberg fails to teach the video driver card of the present invention that executes scrambling/descrambling at the MPEG encoding and decoding process level.

No claim related fees are believed to be due with this response. In the event any such fees are due, please debit Deposit Account 08-2623.

Reconsideration and allowance of the present application is respectfully requested.

Respectfully submitted,

HOLLAND & HART LLP

By: _____

Francis A. Sirr, Esq.
Registration No. 17,265
P.O. Box 8749
Denver, Colorado 80201-8749
(303) 473-2700, x2709

Date: 11/5/04

3298981_1.DOC